DF
DIARIO FINANCIERO®
SUPLEMENTO
SANTIAGO DE CHILE
MARTES 12 DE MAYO DE 2026

LAS TECNOLOGÍAS Y TENDENCIAS QUE ESTÁN AL SERVICIO DE LA PROTECCIÓN DE DATOS

Resolver problemas de visibilidad, trazabilidad y control de datos son algunos de los desafíos en que herramientas como la automatización están tomando fuerza. POR ANAÍS PERSSON

Las empresas están incorporando nuevas capas tecnológicas para responder a una exigencia clave: saber qué datos personales tienen, dónde están, quién accede a ellos y cómo demostrar su correcto tratamiento, cuando faltan pocos meses para la entrada en vigencia de la Ley 21.719 sobre protección de datos personales.

"El principio de responsabilidad proactiva cambia completamente el escenario. Ya no basta con hacer las cosas bien, las organizaciones deben poder demostrarlo", explica el fundador y director de LegalDatos, Daniel Manríquez. En ese contexto, afirma que las herramientas de descubrimiento y mapeo permiten identificar información dispersa en bases de datos, correos, planillas o servicios cloud.

El CEO de Jumpdot, Mauricio Palma, explica que otra capa relevante es la clasificación de datos, que permite distinguir información sensible, como datos biométricos, financieros o de salud, para aplicar resguardo. También se suman tecnologías de trazabilidad, capaces de reconstruir el recorrido de un dato y acreditar bajo qué consentimiento fue obtenido.

La automatización también gana espacio. Según Palma, estas herramientas permiten gestionar solicitudes de acceso, rectificación o eliminación de datos dentro de los plazos que exige la ley. Para Manríquez, ayudan a enfrentar la práctica de acumular información "por si acaso", alertando para eliminar o anonimizar datos antiguos.

Otras necesidad creciente es acreditar cumplimiento. El CIO de Kulvio, Alexis Cona, explica que las empresas requieren generar evidencia auditable para demostrar qué datos se trataron y bajo qué autorización. Agrega que las herramientas de control de accesos e identidades permiten limitar permisos y reducir riesgos de exposición.

Desde Entelgy Chile, su gerente de negocios de ciberseguridad, Pablo Álvarez, advierte que muchas empresas operan con baja visibilidad sobre datos y permisos excesivos, y que herramientas de monitoreo ayudan a detectar configuraciones inseguras.

A estas capas se suman herramientas de autenticación e identidad digital. El gerente general de Ecert, Alfredo Guardiola, sostiene que si una empresa no puede verificar la identidad de quien ejerce sus derechos sobre datos personales, "el proceso completo se vuelve vulnerable".

El nivel de preparación para implementar estas tecnologías sigue siendo desigual, advierten los expertos. Según Palma y Álvarez, sectores como banca, telecomunicaciones, retail y minería avanzan más rápido por exigencias regulatorias y estándares internacionales.

VITRINA EMPRESARIAL

jumpdot.cl

JUMPDOT.CL TE ACOMPAÑA EN ESTE PROCESO:

La forma más práctica de tomarle el pulso a tu empresa frente a la Ley de Protección de Datos Personales

Una forma rápida y simple de empezar es por tu sitio web. Hay tres puntos que pueden servir como primera mirada para entender cómo está tu empresa frente a la ley: formularios, política de privacidad, y cookies o trackers.

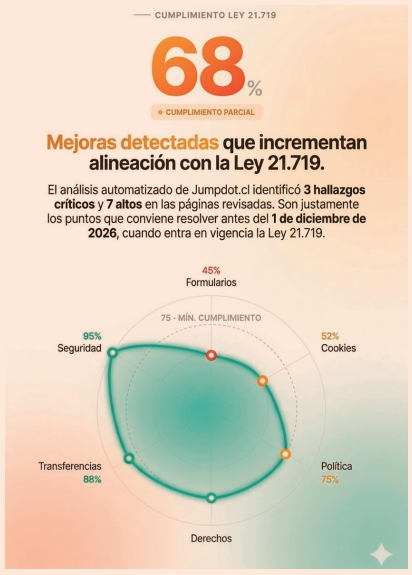
La Ley de Protección de Datos Personales puede parecer amplia y compleja, pero una forma práctica de empezar es mirar lo que la empresa ya tiene publicado: su sitio web. Ahí están algunos de los puntos más visibles donde se capturan, explican o activan datos personales de visitantes y clientes.

Jumpdot.cl propone revisar tres elementos concretos: formularios, política de privacidad, y cookies o trackers. Esta revisión funciona como una primera mirada para entender si la empresa está bien encaminada o si necesita ajustar su forma de informar, pedir aceptación o permitir elección.

El mensaje editorial evita el miedo y la sobrepromesa. La invitación es simple: empezar por lo visible, revisar por cuenta propia o avanzar con apoyo.

Jumpdot acompaña ese proceso desde jumpdot.cl.

Este gráfico de radar (a modo de ejemplo) muestra un servicio de consultoría de Jumpdot.cl con cuatro pilares evaluados, cada uno con 25 puntos a revisar. El pilar mejor evaluado en este caso, es "Formularios", con un cumplimiento de 19 puntos (19/25).



https://jumpdot.cl/

VITRINA EMPRESARIAL

LegalDatos

LA VISIÓN DESDE LEGALDATOS:

La nueva Ley de Protección de Datos Personales impone un cambio legal y cultural crítico para todas las empresas

Como división del estudio jurídico Manríquez Rivera, LegalDatos prepara a empresas y organizaciones para cumplir con la nueva Ley 21.719 de Protección de Datos Personales en Chile, implementa Compliance de Datos y Modelos de Prevención de Infracciones para transformar el riesgo de multas en seguridad estratégica.

"Cuando se habla de datos personales, muchos imaginan que es un asunto estrictamente informático y de ciberseguridad. Hoy en día debemos desmitificar esta visión. Con la nueva Ley 21.719, los datos dejaron de ser un tema puramente tecnológico para convertirse en un desafío legal crítico para todas las empresas. Hablamos de contratos de trabajos, de contratos comerciales, huellas digitales, bases de datos de clientes y hasta correos electrónicos. La ley consagra un cambio cultural", afirma Daniel Manríquez Sansigolo, Director Legal del estudio jurídico especializado LegalDatos.

En dicho contexto, las empresas no son dueñas de esos datos, sino solo un poseedor temporal, para cuyos efectos la Ley 21.719 crea la Agencia de Protección de Datos Personales, órgano autónomo que podrá fiscalizar y aplicar multas de hasta 20.000 UTM. Ya no basta con tener seguridad informática, pues este nuevo cuerpo legal exige demostrar una "responsabilidad proactiva" al respecto, por lo que resulta vital implementar un Modelo de Prevención de Infracciones frente a un riesgo que debería ser innecesario en una compañía del siglo XXI.

Daniel Manríquez Sansigolo, Director Legal del estudio jurídico especializado LegalDatos.

Para responder a tales desafíos, "en LegalDatos blindamos la continuidad operativa de su negocio. Adecuarse toma meses y el reloj ya está corriendo", finaliza Daniel Manríquez.

https://legaldatos.cl

LA HERENCIA DE DATOS QUE COMPLICA A LAS EMPRESAS ANTE LA NUEVA LEY

De cara a la entrada en vigencia de la nueva normativa en diciembre próximo, las organizaciones enfrentan el costo de ordenar bases de datos históricas construidas sin gobernanza clara, con riesgos que van desde multas y litigios hasta problemas operacionales y reputacionales. POR ANAÍS PERSSON

Durante años, las empresas chilenas acumularon información de clientes, trabajadores y proveedores bajo una lógica que pronto quedará obsoleta. Correos electrónicos obtenidos desde formularios web, bases comerciales construidas a partir de campañas antiguas, planillas compartidas entre áreas y datos almacenados indefinidamente pasaron a formar parte de un ecosistema que, con la entrada en vigencia de la nueva Ley de Protección de Datos Personales el próximo 1 de diciembre, se verá puesto a prueba.

El CEO de Jumpdot, Mauricio Palma, sostiene que parte importante del problema sigue estando en los puntos de entrada más básicos. "En algunos casos, los formularios y los pop-ups de 'suscríbete a nuestro newsletter' piden nombre, correo y teléfono sin explicar con claridad para qué se van a usar esos datos, sin un *checkbox* de aceptación expresa o sin un link visible a la política de privacidad", advierte.

No obstante, el gerente general de Fundación País Digital, Fernando Sánchez, afirma que el "talón de Aquiles del cumplimiento" es ordenar décadas de información acumulada. Según explica, muchas organizaciones avanzaron rápidamente en digitalización sin desarrollar una arquitectura clara de gestión de datos. El resultado fueron bases dispersas, duplicadas y administradas por distintas áreas sin trazabilidad completa sobre el origen, uso o eliminación de la información.

Según Víctor Saldaña, fundador de Kulvio y CEO de Solutoria, uno de los principales problemas que aparece en los diagnósticos es la falta de inventario. "Nadie en la organización tiene un mapa completo de qué tablas, qué archivos, qué buzones de correo

VITRINA EMPRESARIAL

Kulvio

OCHO AÑOS DE NORMATIVA EUROPEA. SIETE MESES PARA CHILE:

Cumplir la Ley de Protección de Datos no es tener una política publicada. Es operarla todos los días

- **En 2025, la Agencia Española de Protección de Datos (AEPD) impuso 325 multas por 48 millones de euros. Las más grandes no fueron por mala fe: simplemente por fallas operativas. Chile entra en régimen el 1 de diciembre de 2026.**
- **Para responder a esta inminente exigencia legal, KULVIO -plataforma SaaS chilena desarrollada por Solutoria- reúne ocho módulos integrados, una guía de doce fases, motor de riesgo automático y registro de auditoría inalterable con firma criptográfica, combinando consultoría especializada y plataforma propia.**

Víctor Saldaña, fundador de KULVIO y CEO de Solutoria.

AENA implantó reconocimiento facial en sus aeropuertos en octubre de 2023 sin la evaluación de impacto que exige el Reglamento General de Protección de Datos (RGPD). En 2025, la AEPD le impuso 10 millones de euros de multa, la mayor sanción del año en España.

La Ley 19.628 modificada por la Ley 21.719, entra en vigencia el 1 de diciembre de 2026, con multas de hasta 20.000 UTM y reincidencia de hasta el 4% de los ingresos anuales. "En Chile el problema no es de voluntad ni de presupuesto. Es saber por dónde empezar: qué se trata, dónde está, quién accede y con qué base legal", afirma Víctor Saldaña, fundador de KULVIO.cl y CEO de Solutoria.

La experiencia europea muestra el patrón. En 2025, la AEPD recibió 30.931 reclamaciones -64% más que el año anterior- y describe las grandes infracciones como "problemas sistémicos con riesgos reales y potenciales para todos los clientes". No son incidentes aislados.

Cumplimiento Demostrable	Automatización Inteligente	Diseñado para Chile
✓ Audit trail inmutable SHA-256	✓ Motor de riesgo automático	✓ Ley 19.628 / Ley 21.719
✓ Trazabilidad completa	✓ SLA controlados con alertas	✓ Guía de 12 fases
✓ Reportes PDF/CSV/JSON	✓ Scheduler de tareas	✓ 80 plantillas documentales
✓ Evidencia ante la Agencia	✓ Asistente IA en cada módulo	✓ Motor de reglas legales
✓ Compliance Records	✓ Notificaciones multi-canal	✓ Trust Center público

KULVIO, para un cumplimiento de datos personales con evidencia auditable.

"El cumplimiento operativo se sostiene en cuatro capas: descubrir y mapear los datos, clasificarlos por sensibilidad, gobernar quién accede a qué y con qué base legal, y dejar evidencia auditable de cada acción", explica Alexis Cona, CIO de KULVIO. "Sin esa estructura, una política bien redactada es un documento sin valor".

"Mientras la Agencia chilena consolida sus criterios, las empresas no parten desde cero", explica Ignacia Cano, abogada y delegada de protección de datos de KULVIO. "Los principios del nuevo régimen -responsabilidad proactiva, evaluación de impacto, derechos de los titulares- son equivalentes a los que España aplica desde 2018. El estándar internacional ya existe; lo que falta es ejecución".

KULVIO, plataforma SaaS chilena desarrollada por Solutoria, reúne ocho módulos integrados, una guía de doce fases, motor de riesgo automático y registro de auditoría inalterable con firma criptográfica. Combina consultoría especializada y plataforma propia, desde 8 UF al mes.

Lo que cada organización haga en los próximos meses determinará si llega al 1 de diciembre con un programa que se sostiene en una auditoría, o con una política publicada que no se opera. España ya recorrió ese camino; en Chile tenemos la oportunidad de no repetir sus tropiezos.

https://KULVIO.CL

y qué sistemas SaaS contienen datos personales", sostiene. Esto se traduce en planillas compartidas, bases de marketing antiguas y datos históricos guardados "por si acaso", además de información almacenada en sistemas que ya ni siquiera se utilizan.

A ello se suma el uso de datos obtenidos bajo consentimientos que la nueva normativa ya no admite, y la conservación indefinida de información. Según explica, muchas empresas siguen compartiendo datos con filiales o terceros sin suficiente respaldo y almacenando información durante años simplemente porque nunca se definieron plazos para eliminarla. El problema es que la nueva ley obligará a justificar cuánto tiempo se conservan esos datos y por qué.

"Las organizaciones asumían que si un dato estaba en internet o en un directorio, podían extraerlo y utilizarlo libremente. La nueva ley elimina esto como base de la licitud", explica el fundador y director de LegalDatos, Daniel Manríquez.

"A menos de siete meses de la entrada en vigencia, la ventana para la adecuación es estrecha. Auditorías de datos, definición de responsables, capacitación de equipos y actualización de políticas son trabajos que toman meses, no semanas, y que en muchos casos exigen reasignación de recursos relevantes", afirma Daniel Manríquez, de LegalDatos.

El riesgo de no actualizarse

De acuerdo con lo que establece la nueva normativa, las organizaciones cuentan con un período de transición de 24 meses desde su publicación para ajustar sus bases de datos existentes a la nueva ley.

La norma establece multas de hasta 5.000 UTM para infracciones leves, 10.000 UTM para graves y 20.000 UTM para gravísimas. "El golpe es mayor para la gran empresa: en caso de reincidencia, la sanción puede escalar hasta el 4% de sus ingresos anuales por ventas", añade Manríquez. A ello se suma el riesgo de litigios e indemnizaciones civiles, ya que también establece un régimen de responsabilidad civil frente a eventuales usos indebidos de datos personales.

Pero los expertos advierten que el impacto puede ir mucho más allá de las sanciones. "Una mala gestión de datos puede afectar la continuidad de servicios, la relación con clientes, la confianza de los usuarios y la capacidad de una empresa para trabajar con proveedores, aliados o mercados que ya exigen estándares más altos de privacidad y seguridad", afirma Sánchez.

La falta de gobernanza también incrementa la exposición frente a filtraciones y brechas de seguridad. Según el informe Cost of a Data Breach 2025 de IBM y Ponemon Institute, el costo promedio global de una brecha de datos alcanzó los US$ 4,44 millones entre marzo de 2025 y febrero de 2025, mientras en América Latina llegó a US$ 3,81 millones.

El especialista en ciberseguridad del Grupo Tecnológico ITQ, Jaime Marchant, explica que cumplir implica conformar equipos interdisciplinarios entre áreas legales, tecnológicas y de procesos, además de designar un delegado de protección de datos. También requiere un proceso de limpieza y gobernanza "que puede extenderse entre seis y 18 meses, dependiendo del volumen de información".

"A menos de siete meses de la entrada en vigencia, la ventana para la adecuación es estrecha. Auditorías de datos, definición de responsables, capacitación de equipos y actualización de políticas son trabajos que toman meses, no semanas, y que en muchos casos exigen reasignación de recursos relevantes", concluye Manríquez.

GRUPO DF
DF DF LUN DF MAS DF SUD! SEÑAL DF
CAPITAL ED BIO ED

Director: José Tomás Santa María / **Subdirectora:** Paula Vargas / **Gerente Comercial:** José Ignacio De la Cuadra / **Editora:** Claudia Marín / **Director Creativo y Arte:** Rodrigo Aguayo
Coordinadora: Marcia Aguilar / **Dirección** Edificio Fundadores, Badajoz 45, piso 10, Las Condes, Fono: 2 23391000 / e-mail: buzondf@df.cl / **Impreso por** Gráfica Andes Limitada, que sólo actúa como impresor.

VITRINA EMPRESARIAL

ecert

EL NUEVO CUERPO LEGAL EXIGE UNA MIRADA MUCHO MÁS INTEGRAL:

La responsabilidad no se delega, el desafío de las empresas frente a la nueva Ley de Protección de Datos

- **Con la entrada en vigor de la nueva Ley de Protección de Datos, las organizaciones en Chile enfrentan un cambio estructural en la forma en que gestionan la información de personas y clientes. Más allá del cumplimiento normativo, el nuevo marco legal instala un principio clave: la responsabilidad sobre los datos no se delega, incluso cuando intervienen proveedores tecnológicos o terceros.**
- **Este punto marca un antes y un después en la manera en que las empresas deben abordar la transformación digital, afirman desde ecert, filial de la Cámara de Comercio de Santiago y líder en el mercado nacional en firma electrónica e identidad digital.**

Hoy, muchas organizaciones externalizan procesos críticos como la verificación de identidad, la firma de documentos, la gestión de consentimientos o el almacenamiento de información. Sin embargo, la nueva Ley 21.719 de Protección de Datos Personales es clara en establecer que la responsabilidad sigue recayendo en la organización que decide tratar esos datos, debiendo responder ante eventuales incumplimientos, brechas de seguridad o usos indebidos.

Para Alfredo Guardiola, gerente general de ecert, esto marca un antes y un después en la manera en que las empresas deben abordar la transformación digital: "Delegar tareas no significa delegar responsabilidades. La ley refuerza algo que ya era evidente, las organizaciones deben hacerse cargo de cómo, con quién y bajo qué estándares se tratan los datos de las personas".

Cumplir no es solo implementar tecnología

Uno de los riesgos más frecuentes es asumir que el cumplimiento se logra únicamente con soluciones tecnológicas. La nueva ley exige una mirada mucho más integral, desde la licitud del tratamiento y la minimización de datos, hasta el deber de confidencialidad, el reporte oportuno de vulnerabilidades de seguridad y la realización de evaluaciones de impacto cuando corresponde.

"La elección de proveedores se vuelve crítica", explica Guardiola. "No basta con que una solución funcione; debe permitir a la organización mantener control, evidencia y respaldo frente a sus obligaciones legales".

En este contexto, herramientas como la firma electrónica avanzada adquieren un rol central. No solo por su reconocimiento legal, sino porque permiten asegurar que quien firma

Alfredo Guardiola, gerente general de ecert.

es efectivamente quien dice ser, que los datos o los documentos no han sido alterados y que existe plena validez jurídica frente a terceros.

Privacidad, control y confianza digital

La nueva ley también instala una expectativa creciente por parte de las personas, mayor control sobre sus datos y mayor transparencia en su uso. Esto ha impulsado el desarrollo de mecanismos más sofisticados, como el registro de consentimiento, que se vuelve el primer paso hacia un tratamiento responsable de la información.

Asimismo, soluciones como la Firma Hash responden a un desafío cada vez más relevante: firmar documentos digitales sin tener que ceder datos innecesarios, protegiendo la privacidad desde el origen, asegurando integridad, autenticidad y validez jurídica.

"Hoy las organizaciones quieren avanzar en digitalización sin perder el control de su información. La confianza digital se construye cuando el diseño de los procesos considera la privacidad como un elemento central, no como un agregado posterior", subraya Guardiola.

Cumplimiento como oportunidad

Más que un obstáculo, la nueva Ley de Protección de Datos abre una oportunidad para fortalecer relaciones con clientes, usuarios y ciudadanos. Reglas claras, procesos seguros y decisiones responsables permiten disminuir riesgos, mejorar la gestión interna y consolidar la confianza en cada interacción digital.

Alfredo Guardiola finaliza: "Cumplir no es solo un requisito legal. Es avanzar hacia relaciones basadas en transparencia, control y confianza. Y ese es un activo estratégico para cualquier organización que quiera proyectarse en el largo plazo".